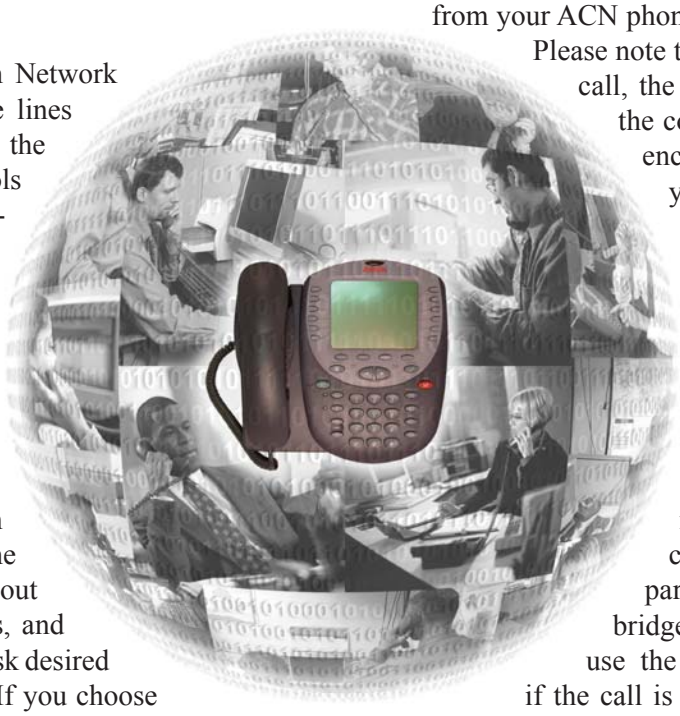
ACN*Report*

Winter 2005 Vol. IV, No. 4

A National Security and Emergency Preparedness (NS/EP) Support Program of the National Communications System

Bridging the Gap

The Alerting and Coordination Network (ACN) specializes in reliable lines of communications. One of the most effective collaboration tools ACN offers is the ACN conference bridge, which can allow up to 165 members to converse simultaneously in a conference call. The following is an overview of standard conference bridge procedures.



Hosting a Conference Call

There are two methods by which you can host a conference call: the Blast-Out method, which blasts out the call to all desired participants, and the Meet-Me method, where you ask desired participants to dial into the call. If you choose the Blast-Out method, you (the host) originate a call from your ACN phone that will blast out to all participants. Please note that before you can initiate a Blast-Out call, the ACN Help Desk must first configure the conference bridge with a preset conference call group. Bearing that in mind, if you need to host a conference call that is time-critical and the ACN Help Desk has not already prepared a preset list, you will have to wait for the Help Desk personnel to configure the bridge before originating the call. In such cases, the Meet-Me option may be more appropriate.

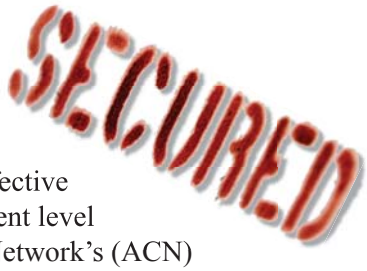
The Meet-Me option is the second means by which you can host an ACN conference call. Via this method, all participants dial into the conference bridge to join the call. It is advisable to use the Meet-Me method to host your call if the call is time-critical and there is not a preset conference group already established.

continued on page 2

In This Issue

According To Policy…

Intrusion Detection



Intrusion detection plays an important role in implementing and enforcing an organizational security policy. As information systems grow in complexity, effective security plans should be able to demonstrate an equivalent level of security assurance. The Alerting and Coordination Network's (ACN) Intrusion Detection Policy provides such assurance.

ACN's Intrusion Detection Policy, which can be obtained from the DHS ACN Program Office, begins at the network's foundation. Its operating system, user accounting, and application software audit logging processes are always enabled on all host and server systems. Each week, ACN administrators review audit logs for servers and hosts on the internal, protected, network. They regularly inspect host-based intrusion tools as well.

ACN security policy calls for robust security software to aide the intrusion detection process. Alarm and alert functions of the ACN firewall and other network perimeter access control systems are always enabled. Network security administrators review,

continued on page 4

ACN News

Public Switched Network

The Alerting and Coordination Network (ACN) has connectivity to the public switched network (PSN). All ACN phones can be reached from the PSN by dialing 703-553 followed by the four-digit ACN extension of the site you are trying to contact.

New Voicemail Message

In February, network engineers transitioned ACN's voicemail service to a new primary voicemail system. As a result of this process, all personal incoming voicemail greetings previously recorded are on the standby voicemail system. If you have not already done so, you will need to rerecord your ACN voicemail greeting. (For steps on how to set up your ACN voicemail greeting, please refer to page 1-11 of the ACN User Manual.)

Sample voicemail greeting:

"You have reached (your organization's name here). Please leave us a message including your organization's name, ACN number, and commercial number. We can also be reached at (your commercial number here). Thank you for calling."

ACN Help Desk Number

The ACN Help Desk has a new toll-free phone number. From this point forward, please dial 1-800-504-4066 when you require Help Desk assistance. The ACN Help Desk offers all members 24/7 customer support.

"Your PIN is your ACN extension followed by the last two digits of your extension a second time."

Monthly Test Results

Each month, ACN administrators conduct two separate phone tests: an individual line ring-down test and a network-wide blast-out test using the ACN conference bridge. The results for the final quarter of 2005 are as follows:

- Ring-down test: 66 percent of all members answered the call, 34 percent did not.
- Blast-out test: 51 percent of all members joined the conference call, 49 percent did not.

Administrators conduct the voice tests on the 15th of every month (if the 15th falls on a weekend, the tests occur the following Monday). ACN administrators send out reminder e-mails to all members one week prior to the tests. Please make every effort to answer the test calls. When answering the blast-out, remember that an automated voice will prompt you to enter your personal identification number (PIN) before joining the call. Your PIN is your ACN extension followed by the last two digits of your extension a second time.

Caller ID

ACN voice over Internet protocol (VoIP) engineers recently modified private branch exchange (PBX) settings in order to support Direct Inward Dialing (DID) and caller identification (ID) display on all network phones. Your caller ID will now appear on the recipient's phone display whenever you originate a call.

Bridging the Gap *continued from page 1*

Connecting Conference Bridges

ACN has two conference bridges (a primary and a secondary). The primary conference bridge can accommodate up to 115 participants at any given time. If you are planning to host an ACN conference call that will involve more than 115 participants, you can start two separate conferences simultaneously (one on each bridge) and then connect both conference bridges, allowing a maximum of 165 participants to join your conference.

Permanent Conference Call Groups

Certain ACN members conduct recurring conference calls and have established permanent conference call groups. Once you establish a permanent conference call group, you no longer need to facilitate future conferences for that group through the ACN Help Desk – you will be able to conduct conference calls at your discretion using the conference group information that the Help Desk provides you. There are several preset groups already established. Please contact the ACN Help Desk for more information.

Monitoring Capabilities

If needed, the ACN Help Desk can monitor conference calls. During the call, the ACN Help Desk views in real-time the dialog status of all participants. It is important to note that the ACN Help Desk cannot listen to the call or hear the content of the discussion. Help Desk personnel are able to monitor participation status only. After you finish hosting a call, feel free to contact the ACN Help Desk and request the status results.

Rootkits & Botnets

Brian Forbes
Senior Technical Writer

Safeguarding your computer has become a full-time job these days. You have to buy all the appropriate firewall and antivirus software. You need to be spy-ware savvy. You must scour the headlines to keep up with telltale warning signs of the latest virus or worm. And just when you think you are on top of the game, a new threat rears its ugly head. Halt a virus, in trots a Trojan Horse. Deep-fry spam, but watch out for the incoming SPIT, too. Let's face it - there is always going to be someone in the hacking community who is up to no good. Yet we should try to look on the bright side. Though the hazards may continue to mount, at least their names keep getting wittier. And on that note, we'll segue to rootkits and botnets.

Rootkits are software programs that hackers install and hide on your system. They are often not inherently damaging themselves; instead, they serve to screen malicious behavior. So, if you contract a rootkit, a hacker could have free reign to root through your system files or record your online activities right under your nose. Methods of contracting a rootkit can vary. Typically, they are able to infiltrate your system unbeknownst to you. For instance, you might download a seemingly harmless software program from the Internet that has a hidden rootkit embedded within. Unmitigated vulnerabilities on your computer can leave you especially susceptible to rootkits.

The biggest difficulty in dealing with rootkits is the fact that they hide on your system and are often undetectable. You likely would not even know your computer was compromised. While traditional antivirus software continues to grow more sophisticated, often times it cannot detect rootkits, in part because they are often clever enough to update themselves, constantly staying one step ahead of the Symantecs and McAfees of the world. Even if you are able detect one of these malicious bugs on your system, getting rid of it is another problem altogether. Simply deleting the offending file might not work, because a rootkit may exist on several files, or on important system files that the rootkit installer has deviously modified.

A botnet, or robot network, simply refers to a network of hacking computers that are controlled externally. Hackers use botnets to spam, expose vulnerabilities, facilitate denial-of-service, pirate information, and other unsavory endeavors. All computers in a botnet can operate simultaneously, so instead of only hacking into one machine at a time, botnet architects can have all the computers in their sinister network infiltrate multiple systems at once. Using numerous computers to commit computer crimes is beneficial to cyber criminals in that it allows them greater range and impact while reducing the likelihood that they'll get pinpointed.

Hackers enlist your machine as part of a botnet by using a conduit, such as a virus, to gain access to your system. Similar to rootkits, a major shortcoming in the war against botnets is the ability to detect them (or lack thereof).

In both cases, issue number one is identification, and issue number two is extermination. Fortunately, proactive measures do exist. As mentioned earlier, antivirus software continues to gain steam in this fight. More and more vendors are developing anti-rootkit products that will hunt down and eliminate these pesky programs. In the case of robot networks, many times a virus is the culprit that makes your computer susceptible to botnet control. A reliable, updated antivirus program in place makes your system a less inviting target.

Antivirus programs aren't the only answer, of course. Sound firewall software is another preventative step worth taking. Firewalls can block much of the unwanted traffic attempting to infiltrate your computer. Ensuring software is up-to-date by installing patches is another way to thwart hackers from exploiting known problems or vulnerabilities. You should always follow safe e-mailing practices as well, in particular regarding attachments. Opening an unexpected attachment from an unknown sender can expose your system to rootkits, botnets, or something worse.

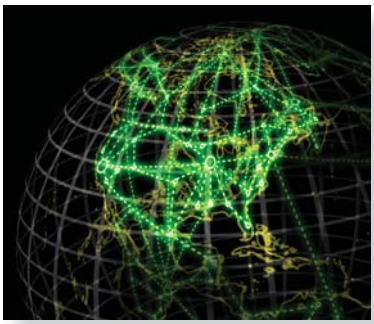
Rootkits and botnets – the names might sound funny, but these two nuisances are nothing to chuckle about. The good news is that, armed with a solid network security plan and some know-how, you can ensure the last laugh belongs to you. :)

Mr. Forbes is a Senior Technical Writer under contract to the NCS.

Did You Know?

Have you ever wondered where your phone number comes from? Contrary to popular belief, the 10 digits are not selected arbitrarily. There is a plan in place that assigns specific phone numbers to your area, your state, your country, and just about everywhere else in North America. It's called the North American Numbering Plan (NANP).

AT&T developed the NANP in 1947 to simplify long distance calling without operator assistance. Four years later, North American countries began implementing the plan. Today, the NANP serves 19 North American countries, including the United States and its territories, Canada, and much of the Caribbean.



All NANP numbers are 10 digits long and consist of a three-digit area code and a seven-digit local number. The North American Numbering Plan Administration (NANPA) is responsible for assigning NANP numbering resources; however, each participating country has ultimate authority over disseminating its own telephone numbers. The NANPA does not create policy; its responsibilities are defined in rules and requirements written by the telecommunications industry and approved by the Federal Communication Commission (FCC). The FCC elects companies to serve five-year terms as the NANPA. NeuStar, the current NANPA acting body, began its tenure in July 2003.

Source: http://www.nanpa.com/

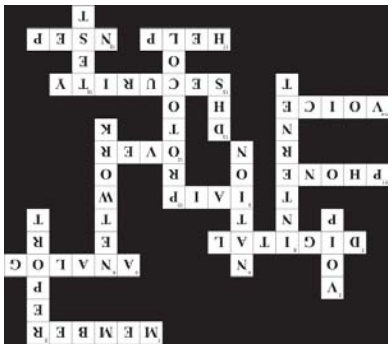
According to Policy *continued from page 1*

audit and log the status and findings of theses systems on a daily basis. In addition, they routinely conduct system integrity checks of the firewall and other network perimeter access control systems.

Diligence by administrators and members alike is a key component of the ACN's Intrusion Detection Policy. Network engineers analyze all issues reported to the ACN Help Desk for symptoms that might indicate intrusive activity. Members are asked to report any signs of wrongdoing or anomalies in system performance to the ACN Help Desk. Any suspected instances of attempted or successful intrusions should be immediately reported.

Violation of this policy may result temporary suspension of user privileges by administrators under direction of Larry Hazzard, ACN Program Manager. Should this occur, the Program Management Team will investigate and determine when to reinstate user privileges.

Last Issue's Mindbender Answer:



ACN Program Management Office

Tel: 1-866-NCS-CALL (1-866-627-2255)
1-703-676-CALL (703-676-2255) DC Metro Area
E-mail: acn@dhs.gov
Web: www.ncs.gov/acn

Department of Homeland Security
Directorate for Preparedness
Cyber Security and Telecommunications
National Communications System
P.O. Box 4502
Arlington, VA 22204-4502

Technical Support: ACN Help Desk

ACN Ext: 4357 (HELP)
Tel: 1-800-504-4066 (Toll Free)
E-mail: smc@arrowhead.com

24/7 ACN Help Desk:
1-800-504-4066

Monthly Test
1:00-1:30 PM EST
15th of the month,
or the following Monday